AU/ACSC/BRIDGES/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

USCYBERCOM

by

Robert T. Bridges, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Colonel Michael P. Linschoten

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
USCYBERCOM	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

Even though the Department of Defense has named cyberspace as the newest domain of warfare, the United States is not adequately organized to conduct cyber war. United States Strategic Command (USSTRATCOM) is the functional combatant command responsible for cyberspace but suffers from numerous problems that prevent it from properly planning, coordinating, and conducting cyberspace operations. Among the problems facing USSTRATCOM are insufficient manning, an overly diverse mission set, and the recent failures within America‟s nuclear enterprise. To overcome USSTRATCOM‟s problems and to provide the cyber domain the prominence needed to properly protect the United States, a new functional combatant command for cyberspace must be established. This command, United States Cyberspace Command (USCYBERCOM), should be given responsibility for conducting worldwide cyber attack, defense, and intelligence. USCYBERCOM should also serve as a supporting command to the geographic combatant commanders and must establish an in-theater headquarters presence similar to the land, air, maritime, and special operations forces. USCYBERCOM personnel should be involved in all phases of campaign planning and ensuring the incorporation of cyber activities throughout all phases of war. The cyberspace domain ignores geographic boarders and will frequently require near-instantaneous attack or defense actions. USCYBERCOM must be given the ability to conduct trans-geographic combatant command and worldwide action and many cyberspace tools can be used in multiple theaters simultaneously. United States Special Operations Command (USSOCOM) provides a model and precedent for a functional combatant command that has an in-theater presence and authority to conduct worldwide operations. The space mission area provides a template for conducting operations with centrally located tools that can have simultaneous multi-theater effects. Combining the USSOCOM and space models into the establishment of USCYBERCOM will greatly enhance the warfighting capabilities of the United States within cyberspace and will better prepare America for the wars of the future.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**39**	

Disclaimer

Preface

As a computer engineer by education and a space operator by training, I requested to join the Warfare in the Cyberspace Domain research elective in hopes of improving my understanding of the newest domain of war. As the seminar progressed, I began to see the parallels between the space and cyberspace domains and the problems these two mission areas face in integrating with the traditional warfare domains. Both space and cyberspace are hailed by leadership as critical to war-fighting efforts but neither has a significant presence in-theater for planning efforts. This paper is an attempt to define what I believe is necessary for cyberspace to achieve full parity as a domain of war. Most of what is discussed also applies directly to the space domain. As I see it, the primary difference between space and cyberspace is that the United States faces peer and near-peer competitors within cyberspace while there is no current true space competitor. Additionally, cyberspace brings numerous offensive and defensive capabilities to today's fight while space is still primarily a force enabler.

While I was researching and writing this paper, the cyberspace community significantly progressed. Between the submission of my first draft and this final report, significant evidence emerged that the DOD is on the verge of establishing a functional combatant command for cyberspace. This paper not only advocates for the establishment of that command; it provides a model for the initial structure of the command and its integration into overall warfighting efforts.

I would like to thank Lt Col Michael Linschoten and Lt Col Mark Black for their assistance in preparing this paper and their mentoring throughout the academic year. I would also like to thank my classmates from both the Cyberspace Seminar and the academic seminars for their support and suggestions to improve this paper. Finally, I would like to thank my wife and the rest of my family for their continuous and overwhelming support.

Abstract

Even though the Department of Defense has named cyberspace as the newest domain of warfare, the United States is not adequately organized to conduct cyber war. United States Strategic Command (USSTRATCOM) is the functional combatant command responsible for cyberspace but suffers from numerous problems that prevent it from properly planning, coordinating, and conducting cyberspace operations. Among the problems facing USSTRATCOM are insufficient manning, an overly diverse mission set, and the recent failures within America's nuclear enterprise.

To overcome USSTRATCOM's problems and to provide the cyber domain the prominence needed to properly protect the United States, a new functional combatant command for cyberspace must be established. This command, United States Cyberspace Command (USCYBERCOM), should be given responsibility for conducting worldwide cyber attack, defense, and intelligence. USCYBERCOM should also serve as a supporting command to the geographic combatant commanders and must establish an in-theater headquarters presence similar to the land, air, maritime, and special operations forces. USCYBERCOM personnel should be involved in all phases of campaign planning and ensuring the incorporation of cyber activities throughout all phases of war.

The cyberspace domain ignores geographic boarders and will frequently require near-instantaneous attack or defense actions. USCYBERCOM must be given the ability to conduct trans-geographic combatant command and worldwide action and many cyberspace tools can be used in multiple theaters simultaneously. United States Special Operations Command (USSOCOM) provides a model and precedent for a functional combatant command that has an in-theater presence and authority to conduct worldwide operations. The space mission area

provides a template for conducting operations with centrally located tools that can have simultaneous multi-theater effects. Combining the USSOCOM and space models into the establishment of USCYBERCOM will greatly enhance the warfighting capabilities of the United States within cyberspace and will better prepare America for the wars of the future.

Table of Contents

> "America is under widespread attack in cyberspace. Unlike in the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battlespace."
>
> General James E. Cartwright
> Former Commander USSTRATCOM[1]

Introduction

The United States is not organized, trained, or equipped to effectively conduct war in cyberspace. United States Strategic Command (USSTRATCOM), the Department of Defense (DOD) command tasked with conducting cyberspace operations, is over-tasked and undermanned to provide the necessary expertise and planning skills necessary to conduct cyberwar. The recent failures in nuclear operations are a further distraction drawing USSTRATCOM's attention away from the cyber mission. To meet current and future threats and war fighter needs, the cyberspace forces must be united under a functional combatant command that is solely focused on cyber warfare.

This command, United States Cyber Command (USCYBERCOM), must be established in such a way as to have equal recognition and responsibility as the other traditional domains of war (air, land, and maritime). To achieve this recognition, USCYBERCOM must establish a presence within the headquarters of each of the geographic combatant commands (GCCs) and applicable joint task forces (JTFs) that is on par with the air, land, maritime, and special operations forces. USCYBERCOM must also be given authority to organize, train, and equip forces with the unique skills, training, and tools necessary for conducting operations in this newest domain of war. Additionally, USCYBERCOM must have the ability and authority to conduct trans-GCC and worldwide operations using tools that are capable of conducting simultaneous inter-theater operations.

The roles, responsibilities, and processes used by USCYBERCOM are not unique. USSOCOM is already tasked with conducting worldwide operations in the Global War on Terror and has authority to organize, train, and equip forces. Establishing a USCYBERCOM presence in theater will allow the command to plug directly into the current joint planning processes. The Joint Space Operations Center model for centralized deconfliction of worldwide operations can be easily adapted for global synchronization of USCYBERCOM operations. USCYBERCOM must strive to become a full partner with the other domains of war and, to do so, must adapt into their processes.

There are methods, other than the establishment of USCYBERCOM, of organizing to operate in the cyberspace environment. The most likely would be to match the Air Force model of combining space and cyberspace into a single functional combatant command. The least expensive would be to provide USSTRATCOM with a small increase in manning and otherwise leave the structure unchanged. While these methods might provide better protection and operational effects than the current arrangement under USSTRATCOM; none would be as effective as granting the domain of cyberspace its own functional combatant command.

Cyberspace Definition

There are multiple definitions of cyberspace that have been used over the last few years that range from describing cyberspace as simply the internet or as expansive as any electromagnetic network or storage medium to "an amorphous entity where information exists and flows."[2] Colonel Gregory Rattray, USAF retired, in his book *Strategic Warfare in Cyberspace*, defines cyberspace as "a man-made environment for the creation, transmittal and use of information in a variety of formats."[3]

For the military, Joint Publication 1-02 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] Vice Chairman of the Joint Chiefs of Staff, General James Cartwright signed a memo defining cyberspace operations as: "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[5]

The joint definitions of cyberspace and cyberspace operations given by General Cartwright and Joint Publication 1-02 provide a starting point for military cyberspace discussions. To understand military action in cyberspace, David Lonsdale defines cyberspace control as "the ability to use the infosphere [cyberspace] for the furtherance of strategic objectives, whilst denying the enemy from doing the same."[6]

To help clarify among the definitions and to establish an operational clarity, USSTRATCOM divides cyberspace into three operational areas: computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE).[7] To relate to more common air and space power terms, CNA is offensive cyberspace, CND is defensive cyberspace, and CNE equates to cyberspace situational awareness. It is these three mission areas, CNA, CND, and CNE that must become the central area of focus of a command focused on cyberspace.

For the purposes of this paper, offensive cyberspace and cyber attack will correspond with the Joint Publication 1-02 definition. Specifically, cyber attack means those activities necessary to deny an enemy access to information technology infrastructures, including

telecommunications networks, the internet, and other computer networks necessary for the conduct of war. Cyber defense will refer to General Cartwright's definition of actions taken to protect military networks and the Global Information Grid.

The Cyber Threat

The United States is under attack in cyberspace. "The 1996 General Accounting Office (GAO) study *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* concluded that 'the hundreds of thousands of attacks that the Defense has already experienced demonstrate that: 1) significant damage can be inflicted by attackers; and 2) attacks pose serious risks to national security.'"[8] In November 2008, "Washington suffered from a severe, painful and widespread attack on the Pentagon's most sensitive computers. The most worrisome aspect was evidence that the attack has official Russian state origins…[This] attack penetrated at least one highly protected and classified DOD network."[9] This attack is just the most recent and most prominent on military computers; it is widely believed that enemy probing and intel gathering events occur on U.S. military computers on a continual basis.

The United States must better recognize and respond to cyberspace threats. In his pamphlet, "50 Cyber Questions Every Airman Can Answer," Dr Kamal Jabbour defines cyber threats by "motivation and intent of the actors."[10] These motivations and intents are: "notoriety" for hackers and crackers, "financial benefit" for criminals, "ideological gain" for terrorists, and "political and military advantage" for nation states.[11] Another potential motivation is found in the "'hacktivists,' [the] technical experts who act independently from governments."[12] These "hacktivists" make themselves out to be patriots that are conducting activities that the government they support cannot or will not carry out.

Computer networks may also be used to further terrorist goals through information operations activities. "In November 2003 at a Yahoo! Groups Web site,…[Muslims were warned] that they should leave three major U.S. cities."[13] This warning "increased public anxiety…without any supporting evidence, detailed information, or materialization of the threats."[14] The terrorist organization Hezbollah developed an online game to recruit new suicide bombers. The game, Special Force, "places the player in various Hezbollah battles with Israeli forces…[and] features a training mode in which participants can practice their shooting skills on Israeli prime minister Sharon and other Israeli political and military figures."[15]

Other nations have also felt the effects of attacks in cyberspace. Following the removal of a WWII Soviet statue from a park, Estonian government officials "expected violent street protests by Estonians of Russian descent."[16] What the officials got instead "was what some here describe as the first war in cyberspace, a monthlong (sic) campaign that has forced Estonian authorities to defend their…nation from a data flood…in retaliation for the removal of the statue."[17] This attack paralyzed government computer networks, interfered with international banking and "overwhelm[ed] the sites of several daily newspapers."[18] The Estonian Defense Minister described the attacks as "a national security situation" and compared the loss of connectivity to "when your ports are shut to the sea."[19] In Denmark, the publishing of "cartoon images of the prophet Mohammed" resulted in "1,000 attacks against web servers."[20] Prior to the conventional attacks of Russia on the Republic of Georgia, "a security researcher…was watching an attack against the country in cyberspace."[21] These attacks "overloaded and effectively shut down Georgian servers."[22] These attacks demonstrate the capabilities of international hackers and the United States faces similar threats in cyberspace.

A larger issue is that of attribution. Due to the nature of the internet, "attackers can mask their identities by using the Internet addresses of others, or remotely program distant computers to send data without their owners even knowing it."[23] It is possible for the United States to face a cyberspace attack from an unknown entity; or worse, to misattribute an attack to and retaliate against an innocent nation.

These examples demonstrate the threats America faces in cyberspace. The U.S. government and American military must be prepared to counter these threats and be prepared to conduct operations to limit the ability and usefulness of enemy networks.

Current Structure

At the combatant command level, USSTRATCOM is currently responsible for cyberspace operations. To carry out this mission, cyberspace has been split into two joint functional commands, JFCC-Network Warfare (JFCC-NW) and the Joint Information Operations Warfare Command (JIOWC), and a joint task force, Joint Task Force-Global Network Operations (JTF-GNO).[24] "JFCC-NW is responsible for deliberate planning of network warfare, which includes coordinated planning of offensive network attack."[25] The JFCC-NW is also responsible for conducting CNA. The JIOWC "is responsible for assisting combatant commands with an integrated approach to information operations…[and it] coordinates network operations and network warfare."[26] JTF-GNO "is responsible for operating and defending the DOD information infrastructure (the so-called Global Information Grid (GIG));"[27] in other words, keeping military computer networks running and conducting CND.

In addition to running their commands, the commander of JFCC-NW also serves as Director of the National Security Agency (NSA) and the JTF-GNO commander is the Director of

the Defense Information Systems Agency (DISA).[28] The NSA serves as the primary government agency for conducting offensive cyberspace activities and CNE with the various military services providing varying levels of internal support and expertise. DISA is the primary intelligence integrator for the DOD and conducts a significant portion of the cyberspace intelligence and exploitation missions.

Within the joint combatant commands and joint task forces, cyber activities are conducted through the information operations cell which is typically designated as J-39.[29] This cell is responsible for all information operations: psychological operations (PSYOP), military deception (MILDEC), operational security (OPSEC), electronic warfare (EW), and computer network operations (CNO).[30] Within the J-39 cell, CNO may be directly represented or may be represented by a USSTRATCOM representative that "participates via collaborative systems or in person when available."[31] This last point exemplifies the need for change. To have a domain of warfare relegated to a single USSTRATCOM member that "participates…in person when available,"[32] shows that the current structure is not prepared to provide the focus on cyberspace that is necessary for future conflicts.

USSTRATCOM

USSTRATCOM is the functional combatant command responsible for "intelligence, surveillance and reconnaissance (ISR), network warfare, global network operations, information operations, integrated missile defense and combating weapons of mass destruction,"[33] as well as conducting space and nuclear operations.[34] Each of these mission areas is global in nature and all have massive national security implications. USSTRATCOM is unique in that it is solely responsible for two domains of war: space and cyberspace. To manage these diverse mission

areas, USSTRATCOM is divided into five joint functional component commands (JFCCs), a standing joint task force, and two centers.[35] For cyberspace operations, USSTRATCOM runs JFCC-NW, JTF-GNO, and the JIOWC. The other agencies within USSTRATCOM are JFCC-Global Strike (JFCC-GS), JFCC-Integrated Missile Defense (JFCC-IMD), JFCC-Space, JFCC-Intelligence, Surveillance, and Reconnaissance (JFCC-ISR), and the USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC-WMD).[36]

JFCC-GS is focused on deterring enemy action and conducting precise and prompt worldwide attack when necessary. The attack may be nuclear using nuclear tipped intercontinental ballistic missiles, conventional or nuclear capable bombers, or submarine launched missiles.[37] JFCC-GS is working with Air Force Space Command to develop a missile with a conventional warhead that could reach intercontinental distances from the United States.[38]

To monitor enemy ballistic missile activity, USSTRATCOM runs JFCC-IMD. JFCC-IMD makes use of space-based assets and ground radars to monitor for missile threats to U.S. interests.[39] The information produced by JFCC-IMD combines with that from SCC-WMD to provide a worldwide picture of WMD threats around the world. SCC-WMD also conducts "contingency and crisis planning to interdict and eliminate the proliferation or use of Weapons of Mass Destruction."[40]

In addition to using space assets to monitor for ballistic missile launches, USSTRATCOM also has a JFCC devoted to space operations. JFCC-Space, is responsible for planning and executing space operations. The goal of this JFCC is to gain space superiority through the use of space control operations and to enhance war fighting capabilities with space assets.[41]

JFCC-ISR is responsible for deconflicting "high priority intelligence requirements. Essentially, ISR helps ensure the best use of resources to provide decision makers and troops with crucial information when and where they need."[42]

These mission areas represent a vast growth in the responsibilities of USSTRATCOM since its inception in 1992. USSTRATCOM was created to take over the operation of nuclear forces following the Air Force's elimination of Strategic Air Command. When the United States Space Command stood down in 2002, USSTRATCOM picked up the space mission and 450 billets to aid in accomplishing the mission. Between 2003 and 2006 the USSTRATCOM was assigned the conventional global strike, ISR, network operations, and combating WMD missions. These new mission areas only brought in a total of 183 additional personnel.[43]

This greatly expanded mission structure setup USSTRATCOM for a loss of focus on nuclear operations. The relative lack of manpower prevents USSTRATCOM from properly manning joint task forces to properly plan and conduct cyberspace operations.

USSTRATCOM Problems

In 2006, "the US military mistakenly sent four nuclear fuses to Taiwan and never caught the error."[44] These fuses were in boxes labeled as helicopter batteries and this mistake went unnoticed until Taiwan complained about not receiving the batteries.[45]

Later that year, a B-52 aircraft traveling from Minot AFB, ND, to Barksdale AFB, LA, were mistakenly loaded with actual nuclear bombs instead of unarmed cruise missiles. These bombs were left on the plane, improperly guarded, for fifteen hours at Minot and another nine hours at Barksdale before they were discovered.[46]

While the nuclear problems seem to be predominately Air Force issues, they relate to bigger issues within America's nuclear enterprise. The Defense Department's Task Force on Nuclear Weapons Management's Phase II report (also known as the Schlesinger Report) "says the Navy and other joint agencies with nuclear responsibilities let the nuclear mission slide after the end of the cold war" and "the lack of interest in and attention to the nuclear mission…goes well beyond the Air Force. This lack of interest and attention have been widespread throughout the DOD and contributed to the decline of attention in the Air Force."[47] USSTRATCOM must focus on rebuilding confidence in the United States' nuclear capabilities since "some of the roughly 30 nations that rely on the U.S. nuclear umbrella…have 'expressed misgivings about whether or not they feel comfortable under the umbrella.'"[48] The Phase II Schlesinger Report goes so far to directly blame problems at USSTRATCOM for the nuclear mistakes:

> With this multiplicity of missions, USSTRATCOM's leadership and staff did not have sufficient time or resources to maintain a singular focus on the nuclear mission. The assumption was that the nuclear mission could sustain itself with less staff oversight while the new missions were being established. In particular, the bomber and cruise missile elements of the nuclear capability lost their priority.[49]

Funding for cyberspace operations within USSTRATCOM is also an issue. "'StratCom (sic) has the UCP (Unified Command Plan) authority [for cyberspace], but the services have the money and that is not the right structure for a warfighting system,' [according to] Vice Adm. (sic) Nancy Brown, the Joint Staff's director for C4 [(command, control, communications, and computers)] systems."[50] The model of having the services provide the money to purchase equipment works for standard systems like tanks, aircraft, and ships but breaks down when applied to the non-traditional systems used in cyberspace. Funding for cyberspace should be overseen by the UCP authority to prevent duplication of efforts and limiting confliction between tools.

Nuclear, space, and cyberspace operations need strong focused leadership and advocacy at the functional combatant commander level. The widespread missions of USSTRATCOM and lack of appropriate personnel and funding prevent it from giving these mission areas the focus they need to successfully lead in all of these areas of operations. Removing the cyberspace mission area from USSTRATCOM would help restore the focus needed on the remaining mission elements.

USSOCOM

USSOCOM is a singularly focused joint command. This organization is responsible to organize, train, and equip special operations forces and as the force provider of special operations forces to the geographical combatant commanders. USSOCOM also has the ability to conduct direct operations anywhere in the world and to cross geographic combatant commander regions when the mission dictates. This global mission with authority to conduct cross-geographic area missions is an ideal model on which to base the construction of USCYBERCOM.

Following the Vietnam War, Special Operations Forces (SOF) funding and capabilities began to erode. The low point in this erosion was the 1980 Desert One attempt to rescue hostages taken at the US embassy in Iran. Poor planning, communication, and weather led to an aborted rescue attempt and the death of eight American troops. [51] This event began a movement to reform SOF. The reform movement was bolstered by the attack on the Marine barracks in Lebanon and with the "command and control problems that occurred during the Grenada invasion."[52] The reform movement culminated in 1986 with Congress passing an amendment to the Goldwater-Nichols Act that "mandated that the President create a unified combatant

command"[53] for SOF. This law setup "a single commander for all SOF promot[ing] interoperability among the forces assigned to the same command,"[54] and resulted in the establishment of the United States Special Operations Command.

USSOCOM is unique among the functional and geographic combatant commands in that it is given the authority to organize, train, and equip forces; tasks that are usually left to the various services. It was the second USSOCOM commander, "General Stiner [who] oversaw the implementation of developing and acquiring 'special operations peculiar' equipment, material, supplies, and services,"[55] in accordance with the Congressional act that established USSOCOM. The USSOCOM mission statement directly reflects these authorities and adds another critical element:

> USSOCOM leads, plans, synchronizes, and as directed, executes global operations against terrorist networks. USSOCOM trains, organizes, equips and deploys combat ready Special Operations Forces to combatant commands."[56]

This additional element is the reference to conducting global operations. USSOCOM has the authority to conduct operations that cross the boarders of the GCCs.

USCYBERCOM

Given all of the problems in the current cyberspace operations construct, the ideal solution is to stand up a new joint functional combatant command, United States Cyberspace Command. Establishing this combatant command would help fulfill one of the recommendations of phase II of the Schlesinger Report:

> The Task Force has concluded that USSTRATCOM does not have the manpower necessary to execute all missions assigned by the current UCP. Given the importance of the nuclear mission, the Task Force recommends that the number of missions assigned to USSTRATCOM be reduced. The Task Force suggests that the missions assigned include deterrence, global strike, and space and that USSTRATCOM continues to be the primary joint enabler for the integrated

> missile defense and combating weapons of mass destruction missions. Reducing the scope of USSTRATCOM's mission would help stabilize its organization and institutionalize the focus required for its core nuclear mission.[57]

A move towards the establishment of a new combatant command is hinted at in the Naval Network Warfare Command Commander's (NAVNETWARCOM) Guidance for 2009. In this guidance, the commander of the Navy's cyberspace forces states, "the current NETWARCOM mission set…already mirrors the mission sets being examined for inclusion in a DoD-level Cyber command."[58]

Additionally, recent rumors within the Pentagon indicate that the establishment of a combatant command for cyberspace may be imminent. According to Colin Clark, a reporter for *DoD Buzz*, "The Pentagon is likely to take the rare action of adding a new combatant commander, this one for cyber warfare."[59] Clark goes on to report, "Defense Secretary Robert Gates has been considering the idea of cyber COCOMs for months and several senior cyberwarfare officials said he is likely to move on this soon."[60]

As an independent domain, cyberspace must be exploited and defended as necessary to support U.S. objectives. "As in other domains, the principles of war and the effects based approach to operations apply."[61] The GCCs must be staffed, educated, and supported to effectively conduct operations in the cyber domain. Cyber operations are inherently global in nature therefore must also be centrally controlled by a functional combatant commander with authority to conduct global operations. USCYBERCOM is the ideal organization to provide this support to the GCCs and to provide overall centralized control.

As a domain of war, cyber should have the same presence in a joint task force or combatant command headquarters as air, land, sea, and special operations. This presence would be similar to that of SOCOM's and would provide the commander with a way to fully integrate

cyberspace operations into his planning. Only with full integration will cyberspace forces be able to provide its full synergistic effects to the warfighter. Cyberspace must have a seat at the Joint Targeting Coordination Board, and be fully involved in campaign planning through all stages of the Joint Operational Planning Process. Cyberspace must be a full participant in joint exercises. It is only through being a full partner and a true player in exercises that cyberspace forces can achieve the full trust and support of air, land, sea, special operations, and space forces.

USCYBERCOM must also unify the three cyberspace mission areas: CNA, CND, and CNE. Having these three mission areas as separate, stovepiped operations greatly increases a number of risks. Prior to any computer network attack, those responsible for conducting the attack must ensure that friendly forces have appropriate defenses against the methods used in the attack. Otherwise, enemy cyber forces could easily co-opt the exploits used by American attackers and turn them on friendly forces. Those conducting attacks must also closely coordinate with those conducting cyberspace intelligence to ensure that a successful attack does not damage or compromise critical intelligence sources.

Attacking and defending in cyberspace requires that military members assigned to USCYBERCOM have access to unique tools and specialized education. Standardization of this education across the services is necessary to provide a common operating picture and basis for coordination. The tools necessary to properly conduct the cyber mission are not unique to each of the services, but should span across the DOD. USCYBERCOM must be given authority and funding, similar to USSOCOM, to organize, train, and equip forces. Allowing USCYBERCOM this authority would streamline cyber training and ensure standardization of tools and operations. To accurately reflect the missions and responsibilities of this proposed command, the following mission statement, based on USOCOM's mission statement is suggested: USCYBERCOM

leads, plans, analyzes, synchronizes, and, as directed, executes offensive global operations against enemy cyberspace networks. USCYBERCOM conducts active defense of U.S. and allied computer networks and trains, organizes, equips, and deploys cyberspace forces to combatant commands.

USCYBERCOM Operations

Cyberspace operations must be fully integrated into planning and operations. "As with the air, land, maritime, and space domains, we leverage dominance in cyberspace to produce militarily useful effects in all domains."[62] The Joint Space Operations Center (JSPOC) has a process that USCYBERCOM can use as a basis for developing this integration.

Due to the global mission of space, space taskings are generated at the theater and JTF levels and are forwarded to the JSPOC. The JSPOC combines and deconflicts taskings from all theaters, adds in any direct JSPOC taskings, and generates a world-wide Space Tasking Order (STO). The JSPOC then sends the theaters and JTF Air Operations Centers (AOCs) their specific portions of the STO. Finally, the AOCs add the STO to their Air Tasking Order (ATO) which is distributed to the operational units for execution. The other functional commanders (JFMCC, JFLCC, etc.) are provided copies of the ATO (with integrated STO) to maintain overall theater awareness and coordination.[63]

The process of developing space taskings outside of theater and then resubmitting them to the AOC for inclusion on the ATO causes problems for those who are concerned about supported/supporting relationships. Having the STO developed outside of theater and integrated into the ATO would seem to imply, for space operations, that the GCC becomes the supporting commander to USSTRATCOM. This is not the case. The GCC responsible for conducting the

operation maintains supported command status as directed in the operations orders. The process used by the JSPOC, and suggested for use by USCYBERCOM, merely establishes a method to coordinate, deconflict, and synchronize worldwide operations of tools that are not inherently limited by geography. This process also gives GCCs access to more tools and weapons than would be possible if direct command and control of space and cyberspace assets were under the direct control of theater or JTF commanders.

Like the space mission set, the missions to be assigned to USCYBERCOM are inherently global in nature. The lack of defined boundaries within cyberspace and the immediacy of response required for many tasks necessitates that global operators in this mission area have the ability to cross geographic borders without waiting for the knowledge and consent of geographic combatant commanders.

To handle the global nature of the mission set, USCYBERCOM must establish a process similar to the JSPOC's for cyberspace taskings. USCYBERCOM should establish a Joint CyberSpace Operations Center (JCSOC) to deconflict and synchronize theater and global taskings. Similar to the JSPOC model, the JCSOC should collect, deconflict, and synchronize theater and global missions onto a world-wide Cyberspace Tasking Order (CTO). This order then would be sent out to the GCCs for inclusion on their ATOs so that all forces in theater have access and insight to the cyber operations. This insight would also allow air, land, sea, and space forces the ability to request adjustments in timing of cyber activities to match with real-world operations delays or events and would enhance synchronization between the warfare domains.

The JCYOC could be collocated with the 24th Air Force to match the 14th Air Force-JSPOC construct or directly located with the USCYBERCOM headquarters. Collocating with the 24th AF would provide an Air Force centric view of operations and may lead to better

integration to the overall AOC process. Attaching the JCYOC directly to USCYBERCOM HQ would increase the "jointness" of the operation and may lead to fewer inter-service rivalry issues, especially since "cyberspace still is not part of DOD Directive 5100.1, an omnibus document covering official department responsibilities and authorities. Thus, neither the Air Force nor any other service has a special claim on it."[64]

USCYBERCOM and the Joint Operational Planning Process

Full integration to the Joint Operational Planning Process is critical for cyberspace to become an equal partner in wartime operations. As a domain of war, cyberspace operations should be pre-planned and synchronized into operational and contingency plans just as the air, land, sea, and space forces are. Cyberspace activities can have significant effects through all campaign phases.

During the shaping phase (phase zero), cyber forces should desensitize the potential enemy to future effects; enemy networks should be probed and vulnerabilities noted; intelligence should be gathered; and friendly vulnerabilities should be studied.[65] These activities will aid in preparing friendly cyber forces to conduct full-scale operations should the conflict progress. These activities should gather as much intelligence as possible so that the tools necessary to exploit enemy networks can be prepared for future operations.

As a campaign moves into the deter phase (phase one), shaping activities should continue. Direct information operations can be executed through the enemy networks in an attempt to deter future undesired actions. Cyberspace could also be used to deny access to command and control or intelligence infrastructures to limit the enemy's ability to conduct operations.

Phase zero and one activities should continue through phases two through five, seize the initiative, dominate, stabilize, and enable civil authority.[66] During phases two, three, and four, actual cyber attacks should be implemented. These attacks could be anything from temporary denial of enemy command and control systems to the shutdown of critical enemy infrastructure (i.e. power grids, dam control systems, telecommunications networks, integrated air defense networks).

Cyberspace is also a major player in several elements of operational design. In most cases cyberspace forces do not suffer from the operational reach limitations that face other forces. Cyberspace effects can be easily timed to simultaneously occur with efforts by other forces. Additionally, cyber operations can be leverage for "JFCs to impose their will on the adversary, increase the adversary's dilemma, and maintain the initiative."[67] Since many cyberspace activities can be conducted from outside of the theater, the JFC can execute these operations without waiting for forces to deploy to the area of operations.

The importance of having unity of command in cyberspace was noted when the mission was first assigned to USSPACECOM. "Placing CNO [Computer Network Operations] under a single operational commander enables unity of command and effort, more efficiently uses available resources, eases coordination with the intelligence community, and establishes clearer interagency coordination."[68]

Cyberspace must have an equal voice when targets are nominated so that the effects of actions conducted in the other domains can be fully understood. The loss of a power grid or telephone switching network may result in the loss of networks that are necessary to conduct cyber operations. Cyber operators must have the ability to inform commanders of potential losses or gains to cyber operations due to action air, land, maritime, and space activities.

USCYBERCOM in the Joint Task Force

USCYBERCOM must be assigned enough forces to fully support geographic combatant commander requirements. When joint task forces are stood up, the commander of the joint task force (CJTF) should designate a joint forces cyber component commander (JFCCC) that is the equivalent of the joint forces land (JFLCC), air (JFACC), maritime (JFMCC), and special operations (JFSOCC) component commanders. The JFCCC "will exercise day-to-day C2 (command and control) of assigned or attached forces" [69] and coordinate execution of missions through the JCYOC. The JCYOC structure, as defined earlier in this paper, would seem to imply that JTF commanders would not be directly assigned forces; however, this is not the case. The JTF must be assigned a planning staff capable of fully integrating cyberspace activities into the JTF's area of operations and, depending on the nature of the operation, deployable cyber teams may be assigned to the JTF to conduct local operations that must be accomplished from within theater.

The establishment of a JFCCC will unify task force efforts amongst the services and provide for centralized reach-back to USCYBERCOM assets. Duplication or interference of cyberspace activities by the other component commanders will be eliminated and the JTF commander will have a single point of contact for cyber planning and execution.

The JFCCC should have an in-theater cyber operations center with a strategy division, a combat plans division, a combat operations division, and an intelligence, surveillance, and reconnaissance division as well as interagency liaisons to the other component commanders.[70] This center would be focused exclusively on JTF operations and would coordinate activities with the JCYOC and facilitate inclusion of the CTO onto the ATO.

Other Alternatives

There are several other options for the future of cyberspace operations. One would be to leave the current structure and let the services advance their cyberspace capabilities as they see fit. Another would be to expand cyberspace forces under USSTRATCOM and to enhance the cyber forces within the GCCs. The most likely option, at least in the short term, is to split the space and cyberspace missions off from USSTRATCOM into their own functional command.

In response to the Schlesinger Report, and the Air Force's roadmap report, "Reinvigorating the Air Force Nuclear Enterprise," the Air Force is in the process of standing up "Global Strike Command [which will bring] the Air Force's intercontinental ballistic missiles [ICBMs] and nuclear capable bombers…under one command."[71] In the process of standing up this command, Air Force Space Command will lose the ICBM mission controlled by 20th Air Force, but will gain the 24th Air Force which is being stood up "in place of the previous plans to create a Cyber Command"[72] within the Air Force. This model of unification of space and cyberspace under a single major command within the Air Force could be carried over to the functional combatant command level.

Moving space and cyberspace out of USSTRATCOM and into their own functional combatant command would fulfill some of the recommendations of the Schlesinger Report. This reorganization would reduce the breadth of mission areas handled by USSTRATCOM and would allow USSTRATCOM to refocus on the nuclear mission. If the DOD does elect to establish a new combatant command, this unification of space and cyberspace in a single command is the most likely scenario. USSTRATCOM must reduce the vast number of mission areas that it handles and the removal of the space and cyberspace missions is probably the most logical

reorganization. It is unlikely that the DOD will attempt to stand up two new functional combatant commands simultaneously due to the costs involved in establishing a command, especially due to the current state of the economy. Therefore it is probable that the establishment of this new command will follow the Air Force's lead and combine space and cyberspace at the combatant command level.

While a combined space and cyberspace combatant command would elevate the prominence of these two mission areas, there are still concerns. First, there is still the problem of having two domains of war combined into a single command. If the DOD is truly going to treat space and cyberspace as domains of war, they should be given equal representation in the GCC and JTF headquarters' staffs. Under a single combatant command, they are likely to be combined. There are also the risks of mismatched focus between the mission areas leading to one being shorted in funding or command level attention. Finally, there is the risk that the rest of the military would begin to think of the two mission areas as being a single mission area and expecting space personnel to be knowledgeable about cyberspace and vice-versa. These are not insurmountable issues, but they should be considered if the DOD chooses this path.

The Air Force and Navy are both in the process of upgrading their cyberspace capabilities. The resulting inherent abilities within the services may provide USSTRATCOM with enough capabilities to mitigate a cyber attack and to effectively conduct offensive cyber operations. The drawbacks to leaving operations within USSTRATCOM are: that the recommendations of the Schlesinger report are not carried out; USSTRATCOM would maintain a divided focus; and the GCCs would not be fully equipped with the cyber expertise needed to properly plan and execute regional cyber war.

Expanding cyberspace forces under USSTRATCOM could achieve several of the same enhancements that a USCYBERCOM would fulfill. The GCCs could be manned with full cyber cells that would be full planning and execution partners. The prime drawbacks continue to be the divided focus within USSTRATCOM and the lack of a clear cyberspace leader.

For Future Research

This paper has focused on the establishment of a component command that focuses exclusively on the military aspects of cyberspace. The definition used by General Cartwright defining cyberspace operations as: "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid,"[73] does not include any reference to civilian networks or infrastructure. If this definition were extrapolated to the other domains of war, it would lead a reader to believe that the military would only fly combat patrols to protect Air Force bases or provide tanks to defend Army posts. While it is well understood that the role of the U.S. military is to protect and defend the American homeland, the role of this military protection in cyberspace has not been defined. The role of USCYBERCOM, or whatever other agency is tasked with military cyberspace operations, must be defined as it relates to civilian networks and computer infrastructure.

This paper also focuses on transferring the cyberspace mission out of USSTRATCOM due to over-tasking and lack of focus. For USSTRATCOM to re-achieve the necessary level of focus on nuclear operations that the Schlesinger report recommends, other USSTRATCOM mission areas should be examined for reassignment. The most notable of these is, the other warfare domain that USSTRATCOM is responsible for, space. The reestablishment of

USSPACECOM must be studied and probably reestablished. Space should also be given the same consideration at the GCC and JTF levels as are recommended for USCYBERCOM.

Another area for future research is the spin-off of the space and cyberspace mission areas into their own separate services. Each of the traditional domains of war has a military service with the primary mission of operating within that domain. Space and cyberspace have personnel within each of the services focused on their mission areas, but the fundamental responsibility of the Army is to win the land battle, of the Navy is to win the sea battle, and of the Air Force is to win the air battle. Until space and cyberspace each have their own service, space and cyberspace personnel will be of secondary priority to their parent services.

Finally, the JSPOC and the recommended JCYOC attempt to conduct operations with worldwide and inter-GCC capabilities through the use of a centralized operational center structure. This structure results in supported/supporting command issues due to the JTF or GCC commander not having full control of assets and operations within his theater and having to request forces to be tasked from outside the area of responsibilitiy. The supported/supporting command relationships and processes in relation to tools with simultaenous inter-GCC and world-wide capabilities must be established in joint doctrine.

Conclusion

Cyberspace is the newest domain of war and the domain where the United States is currently most vulnerable to attack. In fact, the United States faces frequent cyber attacks that have resulted in the compromise of both unclassified and classified systems. To counter these threats, cyber must be elevated out of the J-39 cell and be given equal representation at the GCCs and JTFs as the other domains of war. Standing up a functional combatant command responsible

for cyberspace is the ideal way of properly preparing for future cyber and multi-domain conflicts. The uniqueness of the cyber mission, its worldwide applications, and implications require that USCYBERCOM synchronize and deconflict all cyber activities and that the command be given the ability to operate across GCC boarders in a timely fashion.

Even though USCYBERCOM has unique requirements and missions, the processes for carrying out those missions are well established. USSOCOM acts as the synchronizer for all special operations activities at the JTF, GCC, and inter-GCC levels. The JSPOC conducts worldwide deconfliction for space activities while ensuring visibility into those activities is incorporated in to theater STOs. USCYBERCOM should be established to match the global nature of USSOCOM and establish a tasking process similar to the JSPOC. USCYBERCOM then must assign personnel to each of the GCC to establish itself as a full participant in the Joint Operational Planning Process.

There are several questions raised in this discussion that, due to time and space constraints, are left for future research. These questions range from how to protect civilian cyberspace infrastructure to formalizing the process for supported/supporting command relationships when dealing with tools that have worldwide access. The future of the space mission area is also left as an open question; as is the possibility of establishing independent military services for space and cyberspace.

There are other potential ways to incorporate cyberspace in to future war-fighting efforts. Continuing the current path while enhancing operator skills is the least expensive method but also probably the least effective. Combining the space and cyberspace missions into a single functional command may prove to be an effective solution and is the most likely to occur in the short term. However, combining two domains of war into a single combatant command runs the

risk of dividing the focus of that command and creating problems similar to those encountered by USSTRATCOM. For the United States to dominate in cyberspace a new Functional Combatant Command, USCYBERCOM, must be established.

Glossary

AFB	Air Force Base
AOC	Air Operations Center
ATO	Air Tasking Order
CJTF	Commander, Joint Task Force
COCOM	Component Command
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CTO	Cyberspace Tasking Order
C2	Command and Control
C4	Command, Control, Communications, and Computers
DISA	Defense Information Systems Agency
DOD	Department of Defense
EW	Electronic Warfare
GAO	General Accounting Office
GCC	Geographic Combatant Command
GIG	Global Information Grid
ICBM	Intercontinental Ballistic Missile

ISR	Intelligence, Surveillance, and Reconnaissance
JCSOC	Joint Cyberspace Operations Center
JFACC	Joint Forces Air Component Commander
JFCC	Joint Forces Combatant Command
JFCCC	Joint Forces Cyberspace Component Commander
JFCC-GS	Joint Forces Combatant Command-Global Strike
JFCC-IMD	Joint Forces Combatant Command-Integrated Missile Defense
JFCC-ISR	Joint Forces Combatant Command-Intelligence, Surveillance, and Reconnaissance
JFCC-NW	Joint Forces Combatant Command-Network Warfare
JFLCC	Joint Forces Land Component Commander
JFMCC	Joint Forces Maritime Component Commander
JFSOC	Joint Forces Special Operations Commander
JIOWC	Joint Information Operations Warfare Command
JSPOC	Joint Space Operations Center
JTF	Joint Task Force
JTF-GNO	Joint Task Force-Global Network Operations
MILDEC	Military Deception
NETWARCOM	Network Warfare Command
NSA	National Security Agency
OPSEC	Operational Security

PSYOP	Psychological Operations
SCC-WMD	STRATCOM Center for Combating Weapons of Mass Destruction
SOF	Special Operations Forces
STO	Space Tasking Order
USCYBERCOM	United States Cyberspace Command
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command
WMD	Weapons of Mass Destruction

[1] AFDD 2-11, 1
[2] Lonsdale, *The Nature of War in the Information Age,* 181.
[3] Rattray, *Strategic Warfare in Cyberspace,* 65.
[4] JP 1-02, 141.
[5] Cartwright, "Definition of Cyberspace Operations."
[6] Lonsdale, *The Nature of War in the Information Age,* 185.
[7] Wilson, "Dominating the Electronic Spectrum," 96.
[8] Rattray, *Strategic Warfare in Cyberspace,* 104.
[9] Grant, "The Cyber Menace."
[10] Jabbour, "50 Cyber Questions,"14.
[11] Jabbour, "50 Cyber Questions,"14.
[12] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[13] Weimann, *Terror on the Internet,* 27.
[14] Weimann, *Terror on the Internet,* 27.
[15] Weimann, *Terror on the Internet,* 92.
[16] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[17] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[18] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[19] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[20] Leyden, *Islamist hackers attack Danish sites.*
[21] Markoff, *Before the Gunfire, Cyberattacks.*
[22] Markoff, *Before the Gunfire, Cyberattacks.*
[23] Landler and Markoff, *Digital Fears Emerge After Data Siege in Estonia.*
[24] Wilson, "Dominating the Electronic Spectrum," 96.
[25] Wilson, "Dominating the Electronic Spectrum," 96.
[26] Wilson, "Dominating the Electronic Spectrum," 96.
[27] Wilson, "Dominating the Electronic Spectrum," 96.
[28] AFDD 2-11, 42.
[29] JP 3-13, IV-3
[30] JP 3-13, x.
[31] JP 3-13, IV-6.
[32] JP 3-13, IV-6.
[33] Cartwright, "Statement on United States Strategic Command."
[34] Cartwright, "Statement on United States Strategic Command."
[35] USSTRATCOM, "Functional Components."
[36] USSTRATCOM, "Functional Components."
[37] USSTRATCOM, "Functional Components."
[38] Cartwright, "Statement on United States Strategic Command."
[39] USSTRATCOM, "Functional Components."
[40] USSTRATCOM, "Functional Components."
[41] USSTRATCOM, "Functional Components."
[42] USSTRATCOM, "Functional Components."
[43] Schlesinger, Phase II report, 53.
[44] Roberts, *U.S. Mistakenly Sent Nuclear Missile Fuses to Taiwan,* 1.
[45] Roberts, *U.S. Mistakenly Sent Nuclear Missile Fuses to Taiwan,* 1.
[46] Warrick and Pincus, *Missteps in the Bunker,* 1.
[47] Hoffman, "Two New Nuclear Reports," 12.
[48] Tyson, "Unified Nuclear Command Urged."
[49] Schlesinger, Phase I report, 24.
[50] Clark, "New Cyber COCOM Likely."
[51] USSOCOM *United States Special Operations Command,* 5.
[52] USSOCOM *States Special Operations Command,* 5.

[53] USSOCOM *States Special Operations Command*, 7.
[54] USSOCOM *States Special Operations Command*, 7.
[55] USSOCOM *States Special Operations Command*, 9.
[56] USSOCOM *States Special Operations Command*, 17.
[57] Schlesinger, Phase I report, 24.
[58] Naval Network Warfare Command Commander's Guidance for 2009, 2-3.
[59] Clark, "New Cyber COCOM Likely"
[60] Clark, "New Cyber COCOM Likely"
[61] AFDD 2-11, 2.
[62] AFDD 2-11, 4.
[63] Information in this paragraph was verified by Col Richard Boltz, USAF, Commander ,614 Air Operations Center.
[64] Grant, "The Cyber Menace."
[65] JP-5, IV-34.
[66] JP-5, IV-34.
[67] JP-5, IV-26.
[68] Anderson, U.S. Space Command: Warfighters," 16.
[69] JP 3-33, III-11.
[70] JP 3-33, III-6.
[71] Hoffman, *USAF Unveils Globabl Strike Command.*
[72] Hoffman, *USAF Unveils Globabl Strike Command.*
[73] Cartwright, "Definition of Cyberspace Operations."

Bibliography

Air Force Doctrine Document (AFDD) 2-11, *Cyberspace Operations*, (DRAFT).

Anderson, Edward G. Lt Gen, USA. "U.S. Space Command: Warfighters." *Military Review.* Nov/Dec 2001. http://web.ebscohost.com/ehost/detail?vid=4&hid=117&sid=ac0bdd99-acd8-496d-b185-e2ce8c9a7ff7%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=5847550 (accessed January 28, 2008).

Arwood, Sam. *Cyberspace as a Theater of Conflict: Federal Law, National Strategy and The Departments of Defense and Homeland Security.* Air Force Institute of Technology, 2007.

Cartwright, James E. General. "Statement on United States Strategic Command Before the Strategic Forces Subcommittee, Senate Armed Services Committee." 28 March 2007. http://armed-services.senate.gov/statemnt/2007/March/Cartwright%2003-28-07.pdf (accessed February 8, 2009).

Cartwright, James E., General. "Definition of Cyberspace Operations." *Action Memo.* September 29, 2008.

Clark, Colin. "New Cyber COCOM Likely." March 6, 2009. http://www.dodbuzz.com/2009/03/06/new-cyber-cocom-likely/ (accessed March 24, 2009).

Grant, Rebecca. "The Cyber Menace." *Air Force Magazine* 92, no. 3 (March 2009).

Hoffman, Michael. "Two New Nuclear Reports Offer More Criticism." *Air Force Times*, January 19, 2009, 12.

Hoffman, Michael. *USAF Unveils Global Strike Command.* October 24, 2008. http://www.defensenews.com/story.php?i=3787270 (accessed March 25, 2009).

Jabbour, Dr. Kamal T. "50 Cyber Questions every Airman Can Answer." Wright Patterson Air Force Base, Ohio: Air Force Research Laboratory, 7 May 2008.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001 as amended through 17 October 2008.

Joint Publication (JP) 3-05. *Doctrine for Joint Special Operations.* 17 December 2003.

Joint Publication (JP) 3-05.1. *Joint Spcial Operations Task Force Operations.* 26 April 2007.

Joint Publication (JP) 3-13. *Information Operations.* 13 Feb 2006.

Joint Publication (JP) 3-60, *Joint Targeting*. 13 Apr 2007.

Joint Publication (JP) 5-0. *Joint Operation Planning.* 26 December 2006.

Joint Publication (JP) 3-33. *Joint Task Force Headquarters.* 16 February 2007.

Landler, Mark and John Markoff. *Digital Fears Emerge After Data Siege in Estonia.* May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html (accessed March 25, 2009).

Leyden, John. *Islamist hackers attack Danish sites.* February 9, 2006. http://www.theregister.co.uk/2006/02/09/islamic_defacement_protests/ (accessed March 25, 2009).

Lonsdale, David J. *The Nature of War in the Information Ag--Clausewitzian Future.* New York: Frank Cass, 2004.

Markoff, John. *Before the Gunfire, Cyberattacks.* August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed March 25, 2009).

Montgomery, Dave. "U.S. military braces for cyberspace-age warfare." *Oakland Tribune*, November 26, 2007. http://findarticles.com/p/articles/mi_qn4176/is_20071126/ai_n21127307/ (accessed March 25, 2009).

Rattray, Gregory J. *Strategic Warfare in Cyberspace.* Cambridge, Massachusetts: Massachusetts Institute of Technology, 2001.

Roberts, Kristin. *U.S. mistakenly sent nuclear missile fuses to Taiwan.* Reuters, March 25, 2008. http://www.reuters.com/article/topNews/idUSN2538598920080325 (accessed March 25, 2009.)

Rogin, Josh. "Cartwright: Cyber warfare strategy 'dysfunctional'." *Federal Computer Week*, February 9, 2007.

Schlesinger, James R. "Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management Phase I: The Air Force's Nuclear Mission." September 2008.

Schlesinger, James R. "Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management Phase II: Review of the DoD Nuclear Mission." December 2008.

Strohm, Chris. *Agencies get failing grades on cybersecurity.* December 9, 2003. http://www.govexec.com/story_page.cfm?filepath=/dailyfed/1203/120903c1.htm (accessed January 29, 2009).

Tyson, Ann Scott. "Unified Nuclear Command Urged." *Washington Post*, September 13, 2008: A08. http://mobile.washingtonpost.com/news.jsp?key=277582&rc=na (accessed March 25, 2009.)

USSOCOM/SOCS-HO, ed. *United States Special Operations Command 20 Year History.* MacDill AFB, FL: USSOCOM/SOCS-HO, 2007.

USSTRATCOM. *Functional Components.* http://www.stratcom.mil/default.asp?page= functional_components (accessed 04 February, 2009).

Warrick, Joby and Walter Pincus. "Missteps in the Bunker." *Washington Post*, September 23, 2007: A01. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/22/ AR2007092201447_pf.html (accessed 25 March, 2009).

Weimann, Gabriel. *Terror on the Internet, The New Arena, the New Challenges.* Washington: United States Institute of Peace Press, 2006.

Wilson, Clay. "Dominating the Electronic Spectrum, Information Operations and Cyberwar." *Military Technology*, 2007: 92-97.